Google Inc. et al v. Egger et al Doc. 265

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION	**No. M:06-cv-01791-VRW**
This Document Relates To: *United States v. Rabner, et al.* (07-1324); *United States v. Gaw, et al.* (07-1242); *United States v. Adams, et al.* (07-1323); *United States v. Palermino, et al.* (07-1326); *United States v. Volz, et al.* (07-1396); *Clayton, et al. v. AT&T Communications of the Southwest, Inc., et al.* (07-1187)	**DECLARATION OF LIEUTENANT GENERAL KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY** Courtroom: 6, 17th Floor Judge: Hon. Vaughn R. Walker Hearing: June 14, 2007; 2:00 p.m.

DECLARATION OF LIEUTENANT GENERAL KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY

I, Lieutenant General Keith B. Alexander, do hereby state and declare as follows:

INTRODUCTION

1. I am the Director of the National Security Agency (NSA), an intelligence agency within the Department of Defense. I am responsible for directing the NSA, overseeing the operations undertaken to carry out its mission, and, by specific charge of the President and the Director of National Intelligence, protecting NSA activities and intelligence sources and methods. I have been designated an original TOP SECRET classification authority under Executive Order No. 12958, 60 Fed Reg. 19825 (1995), as amended on March 25, 2003, and Department of Defense Directive No. 5200.1-R, Information Security Program Regulation, 32 C.F.R. § 159a.12(2000). The statements made herein are based on my personal knowledge of NSA activities and operations and on information made available to me as Director of the NSA.

2. The NSA was established by Presidential Directive in 1952 as a separately

Dockets.Justia.com

organized agency within the Department of Defense. Under Executive Order 12333 § 1.12(b), as amended, the NSA's cryptologic mission includes three functions: (1) to collect, process, and disseminate signals intelligence (SIGINT) information, of which communications intelligence (COMINT) is a significant subset, for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) the support of military operations; (2) to conduct information security activities; and (3) to conduct operations security training for the U.S. Government.

3. There are two primary reasons for gathering and analyzing foreign intelligence information. The first, and most important, is to gain information required to direct U.S. resources as necessary to counter external threats. The second reason is to obtain information necessary to the formulation of U.S. foreign policy. Foreign intelligence information provided by the NSA is thus relevant to a wide range of important issues, including military order of battle; threat warnings and readiness; arms proliferation; international terrorism; and foreign aspects of international narcotics trafficking.

4. In the course of my official duties, I have been advised of the lawsuits referenced in the above caption, the state proceedings that are the subject of the lawsuits, and the information sought in those state proceedings. As set forth below, disclosing the information sought in the state proceedings would cause exceptionally grave damage to the national security of the United States.

BACKGROUND OF STATE PROCEEDINGS

5. In particular, I have been advised of the following facts regarding the state proceedings in New Jersey, Missouri, Maine, Connecticut, and Vermont.

A. New Jersey

6. On May 17, 2006, New Jersey state officials sent subpoenas duces tecum entitled "Provision of Telephone Call History Data to the National Security Agency" to Verizon

Communications, Inc., AT&T, Inc., Cingular Wireless LLC, Qwest Communications International, Inc., and Sprint Nextel Corp. The subpoenas demand that the telecommunication companies produce information regarding specified categories of alleged communications between the companies and the NSA since September 11, 2001. The subpoenas purport to be issued pursuant to state law and state that "[f]ailure to comply with this Subpoena may render you liable for contempt of court and such other penalties as are provided by law."

7. The New Jersey subpoenas seek, among other things, (1) "[a]ll names and complete addresses of Persons including, but not limited to, all affiliates, subsidiaries and entities, that provide Telephone Call History Data to the NSA"; (2) "[a]ll Executive Orders issued by the President of the United States and provided to [the Carrier Defendant] concerning any demand or request to provide Telephone Call History Data to the NSA"; (3) "[a]ll orders, subpoenas and warrants issued by or on behalf of any unit or officer of the Executive Branch of the Federal Government and provided to [the Carrier Defendant] concerning any demand or request to provide Telephone Call History Data to the NSA"; (4) "[a]ll orders, subpoenas and warrants issued by or on behalf of any Federal or State judicial authority and provided to [a Carrier Defendant] concerning any demand or request to provide Telephone Call History Data to the NSA"; (5) "[a]ll Documents concerning the basis for [the Carrier Defendant's] provision of Telephone Call History Data to the NSA, including, but not limited to, any legal or contractual authority"; (6) "[a]ll Documents concerning any written or oral contracts, memoranda of understanding, memoranda of agreement, other agreements or correspondence by or on behalf of [the Carrier Defendant] and the NSA concerning the provision of Telephone Call History Data to the NSA"; (7) "[a]ll Documents concerning any communication between [the Carrier Defendant] and the NSA or any other unit or officer of the Executive Branch of the Federal Government concerning the provision of Telephone Call History Data to the NSA"; and (8) "[a]ll Documents concerning any demand or request that [the Carrier Defendant] provide Telephone Call History

Data to the NSA." *See* Document Requests, ¶¶1-13 at Exh. C to *Rabner* Compl.

B. Missouri

8. On June 19, 2006, and June 22, 2006, two Commissioners on the Missouri Public Service Commission sent subpoenas ad testificandum and subpoenas duces tecum to Southwestern Bell Telephone, L.P., SBC Advanced Solutions, Inc., SBC Long Distance, LLC, AT&T Communications of the Southwest, Inc., TCG St. Louis Holdings, Inc., and TCG Kansas City, Inc. These subpoenas purport to be issued pursuant to state law and seek testimony regarding (1) "[t]he number of Missouri customers, if any, whose calling records have been delivered or otherwise disclosed to the NSA and whether or not any of those customers were notified that their records would be or had been so disclosed and whether or not any of those customers consented to the disclosure;" (2) "[t]he legal authority, if any, under which the disclosures . . . were made;" (3) "[t]he nature or type of information disclosed to the NSA, including telephone number, subscriber name and address, social security numbers, calling patterns, calling history, billing information, credit card information, internet data, and the like;" and (4) "[t]he particular exchanges for which any number was disclosed to the NSA." *See* Exh. C to *Gaw* Compl., attachment A, ¶¶ 1-5. The subpoenas also seeks various documents, "[a]ny order, subpoena or directive of any court, tribunal or administrative agency or officer whatsoever, directing or demanding the release of customer proprietary information relating to Missouri customers;" and "[c]opies of all records maintained pursuant to PSC Rule 4 CSR 240-33.160(6) involving the disclosure of CPNI to a third party." *See* Exh. D to *Gaw* Compl., attachment A, ¶¶ 1-4. The subpoenas provide that each company served should fail to comply with the subpoena at their "peril."

C. Maine

9. On May 8, 2006, a group of private individuals asked members of the Maine Public Utilities Commission (MPUC) to "investigate whether and to what extent Verizon New

England Inc. d/b/a Verizon Maine has cooperated with the National Security Agency (NSA) in connection with two alleged intelligence gathering programs." *See* August 9, 2006 Order of the MPUC at 1, attached as Exh. D to *Adams* Compl.; *see also Adams* Compl. ¶ 27. The United States advised the MPUC members that they lacked authority under the Constitution and federal statutes to investigate the alleged foreign-intelligence gathering functions of the United States, and that federal law also preempted their authority. *See Adams* Compl. ¶ 28; *see also* Letter of July 28, 2006 from Peter D. Keisler to Maine State Defendants at 2-6, attached as Exh. C to *Adams* Compl. Nevertheless, on August 9, 2006, the MPUC issued an order that, among other things, seeks to "require that Verizon provide sworn affirmations of representations it made in its filed response to the complaint." Exh. D to *Adams* Compl. at 3.

10. The MPUC Order focuses on public statements of Verizon made in May 2006, shortly after news reports on alleged NSA activities, and seeks information regarding the alleged foreign intelligence gathering activities of the United States and the NSA in an attempt to determine whether Verizon participated in the alleged foreign intelligence gathering program. *See* Exh. D to *Adams* Compl. at 3. The Order purports to require Verizon to make a "sworn affirmation" that other statements are "true and not misleading in light of the circumstances in which [they were] made." *Id.* Among other things, the Order seeks to require Verizon to confirm that: (1) it "was not asked by NSA to provide, nor did [it] provide, customer phone records from any of its businesses, or any call data from those records"; (2) "[n]one of these companies – wireless or wireline – provided customer records or call data"; and (3) it "did not provide to NSA customer records or call data, local or otherwise." *See id.* at 2, 4.

D. Connecticut

11. On May 24, 2006, the American Civil Liberties Union of Connecticut (ACLU) requested that members of the Connecticut Department of Public Utility Control (DPUC), "investigate whether [AT&T Inc., The Southern New England Telephone Company d/b/a AT&T

Connecticut, The Woodbury Telephone Company d/b/a AT&T Woodbury and Verizon New York, Inc.] have disclosed customer information of their customers in Connecticut to the National Security Agency ("NSA") without warrants, court orders or subpoenas." *See Palermino* Compl. ¶ 34. The companies argued that this request should be rejected in light of federal law, but the DPUC refused to dismiss the case in July 2006. The ACLU then sought discovery by issuing interrogatories to AT&T and Verizon. *See* Aug. 10, 2006 ACLU Interrogatories (Exh. C to *Palermino* Compl.); *see also Palermino* Compl. ¶ 35. The companies moved to strike these interrogatories, but again the DPUC denied this motion, stating that the ACLU "should be allowed the opportunity to conduct discovery in support of its claims." *See* August 23, 2006 DPUC Order at 1 (Exh. D to *Palermino* Compl.).

12. In light of the ACLU interrogatories, the DPUC's Order of August 23, 2006, seeks to compel the disclosure of information regarding, *inter alia*, (1) whether the companies "disclosed customer information and/or records to private parties, government entities and/or law enforcement personnel when not compelled to do so by subpoena, warrant, court order or a request under 18 U.S.C. § 2709 ("National Security Letter" or "NSL")"; (2) the "full details of each occasion on which AT&T [and Verizon] disclosed customer information and/or records to private parties, government entities and/or law enforcement personnel when not compelled to do so by subpoena, warrant, court order or NSL, including the date of each request, the information sought, the information provided, and the date on which the information was provided"; and (3) whether "AT&T [and Verizon] had any policy or policies during the Relevant Period, whether written or unwritten, concerning the disclosure of customer information and/or records to private parties, government entities and/or law enforcement personnel when not compelled to do so by subpoena, warrant, court order or NSL." Exh. C to *Palermino* Compl. at 4.

E. Vermont

13. On May 17, 2006, the Vermont Department of Public Service (VDPS) began

investigating the alleged foreign intelligence gathering functions of the United States when the VDPS sent information requests requiring responses to questions about the alleged relationship between the NSA and AT&T Communications of New England, Inc. *See* May 17, 2006 Information Requests (Exh. C to *Volz* Compl.). On June 21, 2006, the VDPS petitioned the Vermont Public Service Board (VPSB) to open an "Investigation into Alleged Unlawful Customer Records Disclosed by AT&T Communications of New England, Inc." *See* June 21, 2006 Letter from Leslie A. Cadwell to Susan M. Hudson at 1 (Exh. D to *Volz* Compl). The VDPS petition purports to use state regulatory power to obtain "information from [the carrier] regarding the alleged disclosure of customer information to the [NSA] and any other state or federal agency." *See id.* at 2, ¶ 2; *see also* ¶¶ 3-6.

14. On June 29, 2006, the VPSB issued an order opening an investigation based on the VDPS complaint. *See* June 29, 2006 Procedural Order of the VPSB (Exh. E to *Volz* Compl.). The VSPB also opened a similar investigation based on allegations against Verizon New England Inc. d/b/a Verizon Vermont. The AT&T and Verizon entities filed motions to dismiss the proceedings, arguing that the federal law preempted the state law underlying the authority of the VPSB. The United States also advised the VPSB by letter that any attempts to obtain information from the telecommunication carriers could not be accomplished without harming national security, and that responses by the carriers would be inconsistent with federal law. *See* July 28, 2006 Letter from Peter D. Keisler to the VPSB (Exh. G to *Volz* Compl.).

15. On September 18, 2006, the VPSB denied the carriers' motions to dismiss, concluding that federal law did not preempt its authority. *See* September 18, 2006 Procedural Order of the VPSB (Exh. H to *Volz* Compl.). On September 21, 2006, the VSPB ordered that AT&T "shall provide an additional response to the information request from the [VDPS] issued on May 17, 2006, under the authority of 30 V.S.A. § 206." *See* September 21, 2006 Procedural Order at 1 (Exh. I to *Volz* Compl.). The Order incorporates, and demands responses to, the May

17, 2006 information requests of the VDPS. *Id.* The Order seeks to compel the carrier to, *inter alia*, (1) state whether it "disclosed or delivered to the [NSA] the phone call records of any [] customers in Vermont at any time since January 1, 2001"; (2) "identify the categories of information [] provided to the NSA, including the called and calling parties' numbers; date of call; time of call; length of call, name of called and calling parties; and the called and calling parties' addresses"; (3) state whether it "disclosed or delivered to any other state or federal agency the phone call records of any [] customer in Vermont since January 1, 2001"; (4) "[s]tate whether the disclosures of [] Vermont customer call information to the NSA and/or any state or federal agency is ongoing" and the "number of occasions" the alleged disclosures occurred; (5) confirm whether it "modified any of its equipment or other physical plant in Vermont to permit access to data and other information carried on its network by any agency of the federal government" and, if so, describe "the location, equipment, and details of such modifications, and state the purpose for permitting such access"; and (6) state whether it "is disclosing records for any communications services other than telephone calling records (e.g. records for e-mail or internet access)." Exh. C to *Volz* Compl. at ¶¶ 1-16.

HARM TO NATIONAL SECURITY POSED BY STATE PROCEEDINGS

16. All five of the state proceedings described above thus seek, at a minimum, information regarding: (1) whether specific telecommunication carriers assisted the NSA with an alleged foreign intelligence program involving the disclosure of large quantities of records pertaining to customer communications; and (2) if such a program exists, the precise nature of the carriers' alleged involvement and details concerning the alleged NSA activities. Such information, however, cannot be disclosed, confirmed, or denied, without causing exceptionally grave damage to the national security of the United States.

17. As a matter of course, the United States can neither confirm nor deny allegations concerning intelligence activities, sources, methods, relationships, or targets. The harm of

revealing such information should be obvious. If it is confirmed that the United States is conducting a particular intelligence activity, that it is gathering information from a particular source, or that it has gathered information by a particular method or on particular persons or matters, such intelligence-gathering activities would be compromised and foreign adversaries, such as al Qaeda and affiliated terrorist organizations, could use such information to avoid detection. Even confirming that a certain intelligence activity or relationship does *not* exist, particularly with respect to specific alleged programs or methods, would cause harm to the national security because alerting our adversaries to channels or groups of individuals that are not under surveillance could likewise help them avoid detection. In addition, denying false allegations is an untenable practice. If the government, for example, were to confirm in certain cases that specific intelligence activities, relationships, or targets do not exist, but then refuse to comment (as it would have to) in a case involving an actual intelligence activity, relationship, or target, a person could easily deduce by comparing such responses that the latter case involved an actual intelligence activity, relationship, or target.

18. With respect to the particular cases at issue, the United States has never confirmed or denied the allegations that form the basis for the five state proceedings: whether the NSA collects large quantities of communication records from certain telecommunication carriers. Confirming or denying such information would disclose whether or not the NSA utilizes particular sources and methods. Such a disclosure would either compromise actual sources and methods or reveal that the NSA does not utilize a particular source or method, in either case providing information that could help an adversary evade detection. Confirming or denying the allegations regarding specific telecommunication companies and specific activities would also replace speculation with certainty for hostile foreign adversaries who are balancing the risk that a particular channel of communication may not be secure against the need to communicate efficiently.

19. Any further elaboration on the public record concerning these matters would reveal information that would cause the very harms that I have identified. To the extent that the Court needs further information regarding these harms, I respectfully refer the Court to the classified declarations that I submitted in support of the state secrets privilege and related statutory privileges (1) on April 20, 2007, in the various other cases against Verizon and MCI before the Court in MDL 06-1791, and (2) on May 12, 2006, in *Hepting v. AT&T,* Case No. 06-672. *See In Camera*, *Ex Parte* Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency, No. M:06-cv-1791 (dated Apr. 20, 2007) (notice of lodging filed at MDL Docket No. 257); *In Camera*, *Ex Parte* Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency, No. 3:06-cv-672 (dated May 12, 2006) (notice of lodging filed at *Hepting* Docket No. 125); *see also In Camera*, *Ex Parte* Declaration of J. Michael McConnell, Director of National Intelligence, M:06-cv-1791 (lodged Apr. 20, 2007) (notice of lodging filed at Docket No. 256); *In Camera*, *Ex Parte* Declaration of John D. Negroponte, Director of National Intelligence, No. 3:06-cv-672 (dated May 12, 2006) (notice of lodging filed at *Hepting* Docket No. 125).

20. Without confirming or denying whether a classified relationships exists between any particular telecommunications carrier and the NSA, and without confirming or denying the existence of any alleged NSA activity, the information demanded in the five state proceedings described above is also protected from disclosure by Section 6 of the National Security Agency Act of 1959 (NSA Act), Public Law No. 86-36 (codified as a note to 50 U.S.C. § 402). Section 6 of the NSA Act provides that "[n]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency [or] any information with respect to the activities thereof . . . ." By this language, Congress expressed its determination that disclosure of any information relating to NSA activities is potentially harmful. The five state proceedings described above seek information related to the alleged

cooperation of telecommunication carriers with alleged NSA activities and specific information about such activities if they exist. Confirming, denying, or describing such information, therefore, is precluded by Section 6 of the National Security Act.

I declare under penalty of perjury that the foregoing is true and correct.

DATE: 26 APR 07

LT. GEN. KEITH B. ALEXANDER
Director, National Security Agency